CERTIFICAT DE CONFORMITE

L'organisme certificateur LSTI

Déclare que le prestataire de service de certification électronique

AGENCE NATIONALE DES TITRES SÉCURISÉS

SIEGE : 33 AVENUE DU MAINE TOUR MAINE MONTPARNASSE 75015 PARIS

Délivre des services de confiance[1] conformes au

Règlement européen 910/2014 du parlement européen et du conseil *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)*

Les services, les certificats et les niveaux certifiés conformes sont détaillés en annexe de la présente attestation.

Ce certificat est enregistré sous le numéro : **Certificate LSTI N° 11001-1095-V1.0**

Ce certificat est basé sur les rapports d'évaluation

LSTI 11001_1095_AS1.1_CONF-_VLSTI_S
LSTI 11001_1235_eidas REval_exigences compl ANSSI transition RGS

Armelle TROTIN
Directrice de la certification

Date de début de validité 20/7/2017
Date de fin de validité 19/7/2019

cofrac ACCRÉDITATION COFRAC N°5-0546 CERTIFICATION DE PRODUITS ET SERVICES PORTÉE DISPONIBLE SUR WWW.COFRAC.FR

[1] eIDAs Art.3(16)

Annexe 1

Schéma de certification

Accréditation

LSTI est accrédité par le Cofrac sous le numéro n°4-0063 selon la norme NF EN ISO 17021, sous le n° 5-0546 selon la norme NF EN ISO/CEI 17065 :2012 et sous le numéro n° 4-0091 selon la norme NF EN ISO/CEI 17024 et selon les règles d'application du Cofrac pour les portées précises disponibles sur le site www.cofrac.fr.
Les certificats de conformité sont émis conformément aux règles générales de la certification des Prestataires de services de confiance (PSC) pour le niveau qualifié LSTI Q054 ou dans le règlement Q055 pour les certifications aux normes européennes listées au paragraphe exigences ci-après.

Contexte réglementaire

La certification de conformité est émise dans le cadre des textes législatifs et réglementaires suivants :

- Règlement européen 910/2014 du parlement européen et du conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)

Et ses actes d'exécution.

Exigences

Pour le niveau « qualifié » les exigences de conformité sont décrites dans les documents suivants les documents de l'organe de contrôle disponibles sur le site www.ssi.gouv.fr :

- **EN 319 403** : Signatures électroniques et infrastructures (ESI) – évaluation des prestataires de services de confiance - Exigences pour les organismes d'évaluation de la conformité évaluant des prestataires de services de confiance.

Et les documents de l'organe de contrôle disponibles sur le site www.ssi.gouv.fr :

- [1] Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet – Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS
- [3] Services d'horodatage électronique qualifiés – Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS

La conformité aux textes cités ci-dessus vaut présomption de conformité aux exigences correspondantes du règlement européen 910/2014 :

- Prestataires de services de confiance qualifiés (articles du règlement (UE) n°910/2014 eIDAS : 5(1), 13(2), 15, 19(1), 19(2), 24(2) a à g, 24(2).j)
- Services d'horodatage électronique qualifiés (articles du règlement (UE) n°910/2014 eIDAS : 24(2).e, 24(2).h et i, 42(1). a à c)
- Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site Internet [articles du règlement (UE) n°910/2014 eIDAS : 24(1), 24(2).e, 24(2).h, 24(2).i, 24(2).k, 24(3), 24(4), 28(1), 38(1), 45(1), 28(4), 38(4), 28(5), 38(5)]

Est vérifiée également la conformité aux normes[2] :

- **ETSI 102 042 V2.4.1** : *Electronic Signatures and Infrastructures (ESI) – Policy requirements for certification authorities issuing public key certificates*
- **ETSI 101 456 V1.4.3 :** *Electronic Signatures and Infrastructures (ESI) – Policy requirements for certification authorities issuing qualified certificates*
- **ETSI 102 023 V1.2.2** *Electronic Signatures and Infrastructures (ESI) – Policy requirements for time-stamping authorities*
- **EN 319 401 V2.1.1**: *Electronic Signatures and Infrastructures (ESI) – General Policy requirements for trust service providers*
- **EN 319 411-1 V1.1.1**: *Electronic signatures and infrastructures (ESI) - Policy and security requirements applicable to trust service providers issuing certificates - Part 1: General requirements*
- **EN 319 411-2 V2.1.1**: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*
- **EN 319 421 V1.1.1**: *Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service providers issuing time- stamps*
- **EN 319 102-1 :** *Electronic Signatures and Infrastructures (ESI) - Procedures for Creation and Validation of AdES Digital Signatures - Part 1: Creation and Validation*
- **ETSI TS 102 640-3:** *Technical Specification Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) : Part 3: Information Security Policy Requirements for REM Management Domains*

Et aux exigences des schéma(s) de certification

- **Q054** - Règlement de certification des prestataires de services de confiance (PSco)- Niveau Qualifié- sur la base d'une qualification RGS
- **Q055** - Règlement de certification des prestataires de services de confiance (PSco)

Résultats de l'évaluation de conformité

- Les services listés en annexe 2 sont délivrés conformément aux exigences listées ci-dessus, en fonction du niveau du service.
- Les exigences de la certification décrites dans le schéma de certification sont respectées.

Acronymes - Services et niveaux

DVCP	Domain Validation Certificate Policy	Authentification serveur
EVCP	Extended Validation Certificate Policy	Authentification serveur
LCP	Lightweight Certificate Policy	Signature-authentification-chiffrement
NCP	Normalized Certificate Policy	Signature-authentification-chiffrement
NCP+	Extended Normalized Certificate	Signature-authentification-chiffrement
OCSP	Online Certificate Status Protocol	
OID	Object IDentifier	
OVCP	Organizational Validation Certificate Policy	Authentification serveur

[2] selon les services offerts par le PSC et le choix des normes ETSI ou EN

QCP public	Certificate policy for qualified certificates issued to the public	Signature
QCP public + SSCD	Certificate policy for qualified certificates issued to the public, requiring use of secure signature-cretaion device	Signature
SSCD	Secure Signature Creation Device	
QCP-l	Policy for EU qualified certificate issued to a legal person	Cachet
QCP-l-qscd	Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD	Cachet
QCP-n	Policy for EU qualified certificate issued to a natural person	Signature
QCP-n-qscd	Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD	Signature
QCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person	Authentification serveur
QSCD	Qualified electronic Signature/Seal Creation Device	
TSA	Time Stamp Authority	Time Stamp
TSAP	Time Stamp Authority Policy	Time Stamp

Annexe 2

Services de certification déclarés conformes

Les services évalués sont caractérisés par les certificats listés ci-après.

CA NAME	Standard	Level (EN 319 411)	serial number (root) OID (end users)	Service
Autorité de certification services applicatifs	ETSI TS 102 042	OVCP	1.2.250.1.200.3.3.7.1.1	Authentification serveur-serveur (A_3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.8.1.1	Authentification serveur-client(A_3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.9.1.1	Cachet serveur (A_3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.10.1.1	Cachet serveur (A_3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.11.1.1	Signature de code (A_3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.12.1.1	Cachet horodatage (A3)
Autorité de certification services applicatifs	ETSI TS 102 042	LCP	1.2.250.1.200.3.3.13.1.1	Confidentialité (A_3)
Autorité de Certification Personnes AAE	ETSI TS 101 456	NCP+	1.2.250.1.200.3.1.1.3.1	Authentification
Autorité de Certification Personnes AAE	ETSI TS 102 042	QCP Public	1.2.250.1.200.3.1.2.3.1	Signature
Autorité de Certification Personnes AAE	ETSI TS 101 456	NCP+	1.2.250.1.200.3.1.4.3.1	Authentification
Autorité de Certification Personnes AAE	ETSI TS 102 042	QCP Public	1.2.250.1.200.3.1.5.3.1	Signature
Acteurs des Collectivités Territoriales	ETSI TS 102 042	NCP+	1.2.250.1.200.2.4.1.2	Authentification
Acteurs des Collectivités Territoriales	ETSI TS 101 456	QCP Public	1.2.250.1.200.2.5.1.2	Signature
Acteurs de l'Administration de l'Etat	ETSI TS 102 042	NCP+	1.2.250.1.200.2.2.1.2	Authentification
Acteurs de l'Administration de l'Etat	ETSI TS 101 456	QCP Public	1.2.250.1.200.2.3.1.2	Signature

Suivi des modifications

Version	Date d'émission	Modification
Version 1	20/7/2017	Initiale certification

FIN DU CERTIFICAT